УДК 004.73
М.Ґіжицкі, Л.Дубчак, Т.Строньскі
(Університет в Бєльску-Бялій (Польща),
(Тернопільський національний економічний університет)

АНАЛІЗ БЕЗПЕКИ ПРОТОКОЛІВ КЕРУВАННЯ КОМП'ЮТЕРНОЮ МЕРЕЖЕЮ

Протокол керування комп'ютерними мережами SNMP (Simple Network Management Protocol), що функціонує на прикладному рівні та належить до сімейства протоколів TCP/IP, часто піддається мережевим атакам, оскільки надає величезні можливості потенціальному зломниснику. Для зчитання або запису якого-небудь об'єкту бази MIB (Management Information Base), яка є набором об'єктів (змінних), що описують мережеві пристрої та їх атрибути, потрібно знати ланцюжок спільноти чи назву, що визначається адміністратором під час конфігурації пристрою. Це становить єдиний захист протоколів SNMPv1 і SNMPv2. На жаль, пакети SNMP не шифруються, тому кожний, хто підслухає таку передачу, може з легкістю одержати ланцюг спільноти. Спільнота визначає комплект змінних, до яких має доступ менеджер. З цією метою визначається режим доступу: для читання (read-only) і для читання та запису (read-write). Можна також надумано задати вигляд для обмеження видимості об'єктів в базі MIB. Слід завжди змінювати ланцюги спільноти для конфігурованих компонентів. Більшість агентів вживають назви "public" в режимі доступу read-only та "private" в режимі read-write. З однієї сторони, це є перевагою, оскільки засоби із задіяним протоколом SNMP підтримують зв'язок з програмним забезпеченням, вживаючи здогадливі уставки. Проте з точки зору безпеки це є недоліком. Якщо надумані значення не будуть змінені, тоді кожний, хто має доступ до мережі через протокол UDP на порті 161, може опитати та змодифікувати змінні, що належать агенту SNMP.

Задачі безпеки розв'язані у третій версії протоколу SNMPv3. В ній введені підходи підтвердження, шифрування та контролю доступу, завдяки чому можна чітко визначити, хто, звідки, до яких об'єктів MIB і з якою метою повинен мати доступ. Для протоколу SNMPv3 вимагається конфігурація двох приватних ключів. Перший з них застосовується для створення цифрового підпису, що забезпечує авторизацію та цілісність даних. Другий ключ використовується для зашифрування відповіді агента за допомогою алгоритму DES в режимі CBC (Cipher Block Chaining). До недоліків протоколу SNMPv3 можна віднести необхідність конфігурації кожного агента перед початком роботи, чого не вимагається в протоколах SNMPv1 і SNMPv2. Проте це є несуттєвим в порівнянні з високим рівнем безпеки.

Стандарт дистанційного моніторингу RMON (Remote Network Monitoring) не вносить жодних змін до протоколу SNMP, хоч був спроектований як доповнення нього, однак значно збільшив його функціональність в сфері керування комп'ютерними мережами. Протокол RMON задає базу MIB дистанційного моніторингу, яка становить доповнення бази MIB-II та надає менеджерові багато істотної інформації про мережу.

Враховуючи розповсюдженість протоколу SNMP, взаємне поєднання програмного забезпечення та пристроїв, а також реалізовані функції, передбачається, що найближчим часом він не припинить бути найпопулярнішим та найефективнішим протоколом менеджменту великих мереж. В майбутньому скоріш всього знадобиться потреба інтеграції SNMP з іншими протоколами та функціями керування мережами. Альтернативи для SNMP можна сподіватися із сторони базованих на мові Java систем та інших нових підходів, які поки що носять дослідний характер.